(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－29844
（P2000－29844A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｃ	５Ｂ０８５
	13/00	３５５		13/00	３５５	５Ｂ０８９

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－192711

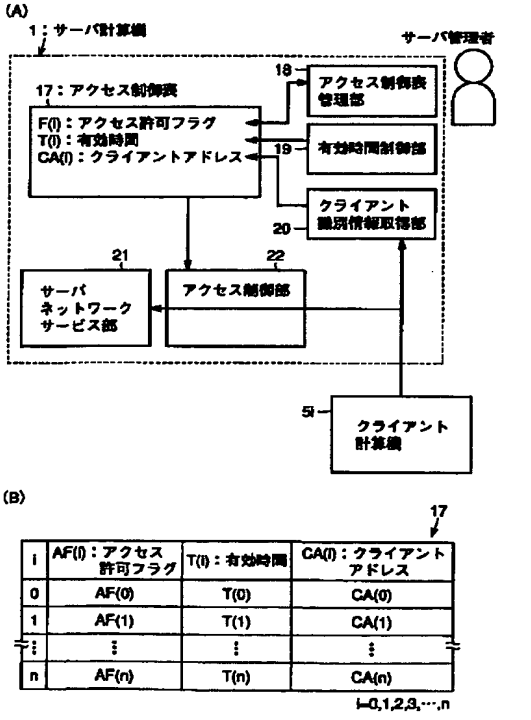
(22)出願日　平成10年７月８日(1998.7.8)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　土居　克良
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(72)発明者　戸田　浩義
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100064746
弁理士　深見　久郎

Ｆターム(参考)　5B085 AC01 AC12 AE04 AE06 BG07
5B089 AA21 AA22 AC03 CC17 DD03
DD07

(54)【発明の名称】　通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置、ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒

(57)【要約】
【課題】　簡単かつ確実に特定クライアント計算機にのみサーバ計算機のアクセスが許可される通信ネットワークの簡易セキュリティ設定方法を提供する。
【解決手段】　サーバ計算機１はアクセス制御表１７を参照しクライアント計算機５ｉのアクセス要求を許可する。表１７には計算機５ｉについて、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されないとオフ設定されるアクセス許可フラグＡＦ（ｉ）と、所定期間内にアクセス要求とともに受信したクライアントアドレスＣＡ（ｉ）とが対応づけて登録される。フラグをオンして所定時間以内にアクセス要求が受信されれば、要求元計算機５ｉに対してのみ、以降のアクセス要求が許可される。



1

【特許請求の範囲】

【請求項１】　１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法であって、

前記クライアント計算機のそれぞれにおいては、個々の識別情報とともに前記サーバ計算機にアクセス要求を送信する送信ステップを備え、

前記サーバ計算機においては、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記クライアント計算機から送信された前記アクセス要求とともに受信した前記識別情報とを対応づけて登録するためのテーブルを有して、

前記アクセス要求を受信したとき、前記アクセス要求とともに受信した前記識別情報と前記テーブルの識別情報とを照合する照合ステップと、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致し、かつ対応のフラグがオン状態である時は、受信された前記アクセス要求を許可するアクセス許可ステップとを備えた、通信ネットワークにおける簡易セキュリティ設定方法。

【請求項２】　前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求項１に記載の通信ネットワークにおける簡易セキュリティ設定方法。

【請求項３】　前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、

前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項１または２に記載の通信ネットワークにおける簡易セキュリティ設定方法。

【請求項４】　１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定装置であって、

前記サーバ計算機において、

前記クライアント計算機のそれぞれから前記サーバ計算機へのアクセス要求を受信したとき、該受信内容から前記クライアント計算機の識別情報を取得する取得手段と、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記取得手段により

2

取得された前記識別情報とを対応づけて登録するためのテーブルと、　前記アクセス要求を受信したとき、前記取得手段により取得された前記識別情報と前記テーブルの識別情報とを照合する照合手段と、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は、受信した前記アクセス要求を許可するアクセス許可手段とを備えた、通信ネットワークにおける簡易セキュリティ設定装置。

【請求項５】　前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求項４に記載の通信ネットワークにおける簡易セキュリティ設定装置。

【請求項６】　前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、

前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項４または５に記載の通信ネットワークにおける簡易セキュリティ設定装置。

【請求項７】　１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法をコンピュータに実行させるための簡易セキュリティ設定プログラムを記録したコンピュータ読取可能な記録媒体であって、

前記簡易セキュリティ設定方法は、

前記クライアント計算機のそれぞれにおいて、個々の識別情報とともに前記サーバ計算機にアクセス要求を送信する送信ステップを備え、

前記サーバ計算機において、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記クライアント計算機から送信された前記アクセス要求とともに受信した前記識別情報とを対応づけて登録するためのテーブルを有し、

前記アクセス要求を受信したとき、前記アクセス要求とともに受信した前記識別情報と前記テーブルの識別情報とを照合する照合ステップと、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は、受信された前記アクセス要求を許可するアクセス許可ステップとを備えた、通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【請求項８】　前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求

項７に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【請求項９】　前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、

前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項７または８に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はサーバ計算機と１台以上のクライアント計算機が相互に通信接続されるような通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体であって、特に、サーバ計算機のサービス提供を特定のクライアント計算機にのみ許可する場合の通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体に関する。

【０００２】

【従来の技術】サーバ計算機がクライアント計算機とネットワークで結合され、クライアント計算機からの要求をサーバ計算機で処理するシステムは、クライアントサーバシステムと呼ばれ、以下のようなさまざまな方法でサービス提供に関するセキュリティの設定を行なっている。これにより、許可されるべき相手にのみサービス提供が許可されて、許可すべきでない相手にはサービス提供が行なわれないようにしている。

【０００３】第１の例として、たとえばサービス提供を許可すべきクライアント計算機のＩＰ（インターネットプロトコルの略）アドレス範囲を事前にサーバ計算機に登録し、これに一致するクライアント計算機のみにサービス提供を許可する方式がある。

【０００４】具体的には“World Wide Web（以下、WWWと略す）サーバ構築技法”インターフェイス１９９５年９月号ｐｐ１５１～１６７においてサーバ計算機に予め記憶されたＩＰアドレスまたはアドレス範囲に一致するアドレスを有するクライアント計算機からの要求のみを受付けてサービス提供を許可する方法がとられていた。

【０００５】たとえば、アドレス範囲パターンが１３３．１５９．＊．＊．であるとき、ＩＰアドレスが１３３．１５９．０．０から１３３．１５９．２５５．２５５までのクライアント計算機にはサービスを許可する。それ以外のクライアント計算機に対してはサービス提供の拒絶通知が行なわれる。

【０００６】第２例としては、たとえばクライアント計算機やサーバ計算機に通信接続する場合に、ユーザ名とパスワードを送信して、サーバ計算機は予め登録されたユーザ名とパスワードに一致する場合にのみアクセス要求を受付ける方式である。

【０００７】具体的には、WWWサーバにおける基本認証方式がこれに当たる。WWWサーバにおける基本認証方式ではクライアント計算機のWWWブラウザがオンしWWWサーバ計算機の特定ページをアクセスしようとすると、ユーザ名とパスワードをクライアント計算機においてユーザに入力させ、予めWWWサーバ側に登録されていたものと一致したときのみ、WWWサーバの特定ページのアクセスを許可するものである。

【０００８】第３例としては、たとえば特開平０２－０５１３９７号公報の回線受信端末装置に示されるものがある。回線受信端末装置として着信応答を許可する加入者番号を記憶しておき、この加入者番号と同じ番号の発信元からの着信だけを受付けることにより、被呼側では希望する発信元との間でだけ通信が行なえる方法が提案される。

【０００９】また第４例として特開平０２－０３６６５７号公報の通信装置がある。この通信装置によれば着信を受付ける相手局の識別情報を記憶しておき、それ以外の相手局からの着信を拒否する方法が提供される。この着信拒否制御を無効化あるいは有効化する機能をもっているため、登録されていない相手局からの着信を面倒な操作なしに拒否可能にする方法が提供される。

【００１０】第５の例として、いわゆる迷惑電話防止システムにも類似の制御方法がある。一般に迷惑電話防止システムの採用する方式は、着信側はかかってきた迷惑電話の直後に電話を操作して電話局に対して所定信号を送信すれば、直前にかかってきた電話番号に対しては以後着信を拒否することができる。これは、電話局側の電話交換機が着信拒否識別番号を記憶するからである。

【００１１】このように通信ネットワークにおけるサーバ計算機に対するクライアント計算機のアクセス制御は、サーバ計算機側に着信許可識別情報を予め登録するか、着信拒否識別情報を予め登録する方法が一般的である。

【００１２】

【発明が解決しようとする課題】ところが、上述したようなアクセスを許可する（着信を許可する）クライアント計算機の識別番号（ＩＰアドレスパターン）を予めサーバ計算機側に登録する方法では、クライアント計算機のＩＰアドレスが予め判明していなければならず、また、その識別情報であるＩＰアドレス値をサーバ計算機に登録しておく必要がある。

【００１３】この場合、サーバクライアントシステムの利用者は、ＩＰアドレスの概念を理解し数値で指定する

必要があり煩わしいという課題があった。これに関し、第５例では機械的に発信者識別番号を記憶させることで、以後着信許可／拒否が行なわれることで数値入力操作が不要となっている点で改善がみられる。

【００１４】また、第２例のような基本認証方式では、クライアント計算機においてユーザ名とパスワードをユーザに入力させる煩雑な操作が必要であるという課題が残る。

【００１５】また、第３および第４例の通信装置では、発呼側をクライアント計算機、着信側をサーバ計算機とすればサーバクライアントシステムのアクセス制御とみなせる。この場合、識別情報はアドレスに相当する。

【００１６】また、上述の第４例では、予め着信応答する加入者番号を記憶しておくので第１例と同等である。

【００１７】また、第５例では第１例同様アクセス許可されるクライアントのアドレスをサーバ側に登録しておく方式と同じであり、許可クライアント計算機のアドレスの事前登録が必要となっている。

【００１８】第４例では着信許可する相手局の識別情報を予め登録する方式であるため、登録以外の局からかかってきた着信を拒否するので第１例に類似している。

【００１９】第４例では着信拒否制御を無効にする手法を使って着信許可に切換える対応をとる必要がある。

【００２０】それゆえにこの発明の目的は、簡単かつ確実に、特定のクライアント計算機に対してのみサーバ計算機へのアクセス要求が許可されるような通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体を提供することである。

【００２１】

【課題を解決するための手段】請求項１に記載の通信ネットワークにおける簡易セキュリティ設定方法は、１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおいて適用されて、以下のような特徴を有する。

【００２２】クライアント計算機のそれぞれにおいては、個々の識別情報とともにサーバ計算機にアクセス要求を送信する送信ステップを備える。

【００２３】サーバ計算機においては、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内にクライアント計算機から送信されたアクセス要求とともに受信した識別情報とを対応づけて登録するためのテーブルを有して、照合ステップと、アクセス許可ステップとを備える。

【００２４】照合ステップはアクセス要求を受信したとき、アクセス要求とともに受信した識別情報とテーブルの識別情報を照合する。

【００２５】アクセス許可ステップは、照合ステップによる照合の結果において、テーブルの識別情報が空または両識別情報が一致し、かつ対応のフラグがオン状態である時は、受信したアクセス要求を許可する。

【００２６】請求項１に記載の通信ネットワークにおける簡易セキュリティ設定方法によれば、サーバ計算機側でフラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラグはオフされるから、所定期間内で最先にサーバ計算機に対してアクセス要求を送信したクライアント計算機に対してのみ、それ以降サーバ計算機側でそのアクセス要求が許可される。

【００２７】したがって、サーバ計算機においてクライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要がなく、サーバ計算機では簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することができるような通信ネットワークにおけるアクセス許可に関するセキュリティを得ることができる。

【００２８】また、一旦アクセス要求が許可されたクライアント計算機側では、サーバ計算機へのアクセス要求時にはパスワードなどの入力が不要となり、ユーザの使い勝手は向上する。

【００２９】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたこと、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、サーバ計算機には所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるというこの方法では、アクセス要求時にユーザはアドレスの概念を知る必要はなく使い勝手が向上する。

【００３０】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作してアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグはオフされるから、他のユーザによりクライアント計算機が操作されて不正にサーバ計算機側がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティは保障される。

【００３１】請求項２に記載の通信ネットワークにおける簡易セキュリティ設定方法では、請求項１に記載の方法におけるテーブルの内容が、外部からの入力内容に基づいて変更可能である。

【００３２】請求項２に記載の簡易セキュリティ設定方法によれば、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【００３３】それゆえに、たとえば、テーブルの識別情

報またはフラグをユーザの所望するように変更できて、通信ネットワークにおいてサーバ計算機でアクセス要求が許可されるクライアント計算機を容易に設定または変更できる。言い換えれば、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容がユーザの所望に応じて容易に設定および変更できる。

【００３４】請求項３に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項１または２に記載の簡易セキュリティ設定方法において、識別情報が、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含む。そして、照合ステップによる照合結果における両識別情報が一致したときとは、両アドレス情報がそれぞれ一致したときである。

【００３５】請求項３に記載の通信ネットワークにおける簡易セキュリティ設定方法によれば、照合ステップにおいてアドレス情報の二重チェックが行なわれ、その結果によってクライアント計算機のサーバ計算機に対するアクセス要求が許可されるか否かが決定される。

【００３６】それゆえに、アドレス情報の二重チェックにより不正なアクセス要求が許可されることは確実に回避されるから、簡単にセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【００３７】請求項４に記載の通信ネットワークにおける簡易セキュリティ設定装置は、１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおいて適用されて、以下のような特徴を有する。

【００３８】サーバ計算機においては、クライアント計算機のそれぞれからサーバ計算機へのアクセス要求を受信したとき、該受信内容からクライアント計算機の識別情報を取得する取得手段と、テーブルと、照合手段と、アクセス許可手段とを備える。

【００３９】テーブルには、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内に取得手段により取得された識別情報とが対応づけて登録される。

【００４０】照合手段は、アクセス要求を受信したとき、取得手段により取得された識別情報とテーブルの識別情報とを照合する。

【００４１】アクセス許可手段は、上述の照合の結果において、テーブルの識別情報が空または両識別情報が一致して、かつ対応するフラグがオン状態である時は、受信したアクセス要求を許可する。

【００４２】請求項４に記載の簡易セキュリティ設定装置によれば、フラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラグはオフされるから、所定期間内で最先にサーバ計算機にアクセス要求を送信したクライアント計算機に対してのみそれ以降、そのアクセス要求がサーバ計算機側で許可される。

【００４３】それゆえに、サーバ計算機において、クライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要がなく、サーバ計算機では簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することを保証するような通信ネットワークにおけるセキュリティを設定できる。

【００４４】また、一旦アクセス要求が許可されたクライアント計算機においてもサーバ計算機へのアクセス要求時には、パスワードなどの入力は不要となってユーザの使い勝手が向上する。

【００４５】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたこと、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるという上述の方法では、アクセス要求時にユーザはアドレスの概念を知る必要がなく使い勝手が向上する。

【００４６】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作してアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグはオフされるので、他のユーザによりクライアント計算機が操作されて不正にサーバ計算機がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティは保障される。

【００４７】請求項５に記載の通信ネットワークにおける簡易セキュリティ設定装置は、請求項４に記載の簡易セキュリティ設定装置におけるテーブルの内容が、外部からの入力内容に基づいて変更可能であるよう構成される。

【００４８】請求項５に記載の簡易セキュリティ設定装置によれば、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【００４９】それゆえに、たとえばテーブルの識別情報またはフラグをユーザの所望するように変更できて、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容を容易に設定または変更できる。

【００５０】請求項６に記載の通信ネットワークにおける簡易セキュリティ設定装置は、請求項４または５に記載の簡易セキュリティ設定装置における識別情報が、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含む。

【００５１】そして、上述の照合手段による照合結果に

おける両識別情報が一致したときとは、この両アドレス情報がそれぞれ一致したときであるよう構成される。

【００５２】請求項６に記載の通信ネットワークにおける簡易セキュリティ設定装置によれば、照合手段のアドレス情報の二重チェックの結果に従ってアクセス許可手段がアクセス要求を許可するか否か決定するから、不正なアクセス要求を許可することが回避される。

【００５３】これにより、簡単にセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【００５４】請求項７に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体は、簡易セキュリティ設定プログラムが、１台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法をコンピュータに実行させるためのものである。

【００５５】この簡易セキュリティ設定方法は、クライアント計算機のそれぞれにおいて、個々の識別情報とともにサーバ計算機にアクセス要求を送信する送信ステップを備える。

【００５６】サーバ計算機においては、照合ステップとアクセス許可ステップとを備える。照合ステップは、アクセス要求を受信したとき、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内にクライアント計算機から送信されたアクセス要求とともに受信した識別情報と対応づけて登録するためのテーブルを参照して、アクセス要求とともに受信した識別情報とこのテーブルの識別情報を照合する。

【００５７】アクセス許可ステップは、照合ステップによる照合の結果において、テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は受信したアクセス要求を許可する。

【００５８】請求項７によれば、サーバ計算機でフラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラグはオフされるから、所定期間内で最先にサーバ計算機に対してアクセス要求を送信したクライアント計算機に対してのみそれ以降、そのアクセス要求がサーバ計算機側で許可される。

【００５９】したがって、サーバ計算機においてクライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要はなく、サーバ計算機においては簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することを保証するような通信ネットワークにおけるセキュリティを構築できる。

【００６０】また、一旦アクセス要求が許可されたクライアント計算機側においても、サーバ計算機のアクセス要求時にはパスワードなどの入力は不要となって、ユーザの使い勝手は向上する。

【００６１】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたことを、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるというこの方法では、アクセス要求時にユーザはアドレスの概念を知る必要がなく使い勝手が向上する。

【００６２】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作しアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグがオフされるので、他のユーザによりクライアント計算機が操作され不正にサーバ計算機がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティが保障される。

【００６３】請求項８に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項７に記載の方法のテーブルの内容が、外部からの入力内容に基づいて変更可能であるよう構成される。

【００６４】これにより、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【００６５】それゆえに、たとえばテーブル上の識別情報またはフラグをユーザの所望するように変更できて、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容をユーザの所望に応じて容易に設定または変更できる。

【００６６】請求項９に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項７または８に記載の方法における識別情報は、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含んで、照合ステップによる照合結果で両識別情報が一致したときとは、この両アドレス情報がそれぞれ一致したときであるよう構成される。

【００６７】これにより、照合ステップによりアドレス情報の二重チェックが行なわれて、アクセス許可ステップはその結果に従ってアクセス要求を許可するか否か決定するので、不正なアクセス要求を許可することが回避される。

【００６８】これにより、簡単にアクセス許可に関するセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【００６９】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照し詳細に説明する。

【００７０】図１（Ａ）と（Ｂ）は、この発明の実施の形態によるサーバ計算機１の機能構成とアクセス制御表とを示す図である。

【００７１】図２は、この発明の実施の形態による通信ネットワークの構成図である。図２において、通信ネットワークは通信回線、たとえばイーサーネットと、サーバ計算機１とイーサーネットを介してサーバ計算機１から各種のサービスが提供され得る複数のクライアント計算機５ｉ（ｉ＝０、１、２、３、…、ｎ）を含む。

【００７２】図示されるように、クライアント計算機５ｉはアクセス要求の発呼側であり、サーバ計算機１はアクセス要求の着呼側である。

【００７３】図３は、図２のサーバ計算機１のブロック構成図である。図３においてサーバ計算機１は、計算機１自体を集中的に制御および管理するためのＣＰＵ１１、各種データおよびプログラムを格納するためのメモリ１２、たとえばハードディスクまたはフラッシュメモリなどからなり各種ソフトウェアおよび後述するアクセス制御表１７を格納するための不揮発メモリ１３、たとえばキーボードおよびマウスなどからなり外部操作されてデータを入力するための入力部１４、たとえばＣＲＴまたは液晶などからなる表示部１５、イーサーネットと該サーバ計算機１とのインターフェイスであるネットワークＩ／Ｏ１６およびこれら各部を接続するバス１０を含む。

【００７４】サーバ計算機１におけるネットワークＩ／Ｏ１６を介したクライアント計算機５ｉへのサービス提供は、不揮発メモリ１３からサーバ用のソフトウェアがメモリ１２に読込まれて、ＣＰＵ１１の制御の下に実行制御されることにより実現される。

【００７５】図１（Ａ）にはサーバ計算機１の機能構成が示され、図１（Ｂ）には図１（Ａ）に示されるアクセス制御表１７の構成例が示される。

【００７６】図１（Ａ）においてサーバ計算機１は接続される各クライアント計算機５ｉに関する該サーバ計算機１に対するアクセス要求を制御するための情報が格納されるアクセス制御表１７、アクセス制御表１７に関連のアクセス制御表管理部１８、有効時間制御部１９、クライアント識別情報取得部２０およびアクセス制御部２２、ならびにサーバネットワークサービス部２１を含む。

【００７７】アクセス制御表１７は図１（Ｂ）に示されるようにクライアント計算機５ｉのうちサーバ計算機１に同時に接続してサービス提供を受けることができる所定台数分のクライアント計算機５ｉのそれぞれに対応して識別情報であるクライアントアドレスＣＡ（ｉ）、該サーバ計算機１へのアクセス要求の許可／不許可を示すアクセス許可フラグＡＦ（ｉ）および有効時間Ｔ（ｉ）をデータ配列にして含む。

【００７８】アクセス許可フラグＡＦ（ｉ）はアクセス要求の許可／不許可をオンまたはオフのブール型変数で示し、有効時間Ｔ（ｉ）は秒単位の変数である。クライアントアドレスＣＡ（ｉ）は整数型の変数であり、ここでは説明を簡単にするためにＩＰアドレス（ＴＣＰ／ＩＰ）の４オクテッドアドレスを使用するが、イーサーネットのＭＡＣ（ｍｅｄｉａ　ａｃｃｅｓｓ　ｃｏｎｔｒｏｌ）アドレスであってもよい。

【００７９】アクセス許可フラグＡＦ（ｉ）の初期値はオフであり、有効時間Ｔ（ｉ）の初期値は０であり、クライアントアドレスＡ（ｉ）の初期値は空である。

【００８０】アクセス許可フラグＡＦ（ｉ）は、サーバ計算機１の管理者が入力部１４を操作することによりオン（許可）オフ（不許可）設定される。

【００８１】アクセス許可フラグＡＦ（ｉ）はオフからオンに設定されると、その後一定時間オン状態が維持される。

【００８２】有効時間Ｔ（ｉ）は対応のアクセス許可フラグＡＦ（ｉ）がオン状態に維持されているべき残り時間を示す。

【００８３】アクセス制御表管理部１８はサーバ計算機１の管理者がアクセス制御表１７を表示部１５に表示しながら入力部１４を操作してアクセス制御表１７の内容を更新（データの書込、消去および変更）するのを制御する。

【００８４】有効時間制御部１９は有効時間Ｔ（ｉ）を設定および更新しながら対応のアクセス許可フラグＡＦ（ｉ）をオフに設定する。

【００８５】詳細には、アクセス許可フラグＡＦ（ｉ）がサーバ管理者によりオフからオン設定されると、対応の有効時間Ｔ（ｉ）に前述の一定期間を示す値を設定して、その後計時しながら有効時間Ｔ（ｉ）を減算して更新する。有効時間制御部１９は減算により有効時間Ｔ（ｉ）が０になると、対応するアクセス許可フラグＡＦ（ｉ）をオンからオフにセットする。

【００８６】クライアント識別情報取得部２０は、サーバ計算機１に対してアクセス要求したクライアント計算機５ｉのアクセス要求とともに受理する識別情報を取得して、クライアントアドレスＣＡ（ｉ）としてアクセス制御表１７に設定する。

【００８７】アクセス制御部２２はサーバ計算機１にアクセス要求したクライアント計算機５ｉについて、アクセス制御表１７の内容に基づいてサーバ計算機１に対するアクセス許可または不許可を制御する。

【００８８】サーバネットワークサービス部２１はアクセス要求したクライアント計算機５ｉが要求するサービス内容を認識して、要求されたサービスをクライアント計算機５ｉに提供する。

【００８９】図４は、この発明の実施の形態によるサーバ計算機１におけるクライアント計算機５ｉからのアクセス要求の許可／不許可を制御するための手順を示すフ

ローチャートである。

【００９０】図５は、図４のフローチャートに従う処理に並行して実行される有効時間Ｔ（ｉ）の減算処理のフローチャートである。

【００９１】図４と図５のフローチャートは予めプログラムにしてメモリ１２にストアされＣＰＵ１１の制御の下に実行される。

【００９２】図６は、この発明の実施の形態によるサーバ計算機１において一定の有効時間Ｔ（ｉ）内にクライアント計算機５ｉのアドレス学習が行なわれた場合の動作を示すタイミングチャートである。

【００９３】図７は、この発明の実施の形態によるサーバ計算機１において、一定の有効時間Ｔ（ｉ）内にクライアント計算機５ｉのアドレス学習が行なわれなかった場合の動作を示すタイミングチャートである。

【００９４】なお、アドレス学習とは、クライアント計算機５ｉのＩＰアドレスなどの識別情報がクライアントアドレスＣＡ（ｉ）としてアクセス制御表１７に登録される動作をいう。

【００９５】図８～図１３は、この発明の実施の形態によるクライアント計算機５ｉとサーバ計算機１間の通信に伴って更新されるアクセス制御表１７の内容の第１～第６例を示す図である。

【００９６】図１４は、この発明の実施の形態によるアクセス制御表１７の書換を説明する図である。

【００９７】サーバ管理者は、アクセス制御表１７の内容を設定または変更するために書換えようとする場合、入力部１４を操作する。この操作に応じてアクセス制御表管理部１８は不揮発メモリ１３からアクセス制御表１７を読出して表示部１５に図１４のように表示する。

【００９８】この表示内容を見て、サーバ管理者は入力部１４を操作し、アクセス制御表１７の内容を所望するように設定または変更することができる。

【００９９】図１４では、矢印のマウスカーソルで、許可フラグＡＦ（ｉ）を示す許可チェックＢＯＸ（左端）にチェック印を入れると、対応するクライアントアドレス（１２３．４５．６７．８９）のアドレス学習が可能となる。また、アドレスリセット（右端）をチェックすると対応するクライアントアドレスＣＡ（ｉ）に関するアドレス学習の内容が消去される。なお、アクセス制御表１７のクライアントアドレスＣＡ（ｉ）の内容は、マウスカーソルとキーボードを併用して修正変更することも可能である。

【０１００】次に、図４と図５を参照しながら、図１のサーバ計算機１におけるクライアント計算機５ｉのアクセス要求の制御に関して説明する。

【０１０１】まず、サーバ計算機１が電源投入されて初期状態にあるとき、アクセス制御表管理部１８はアクセス制御表１７に初期値を設定する。

【０１０２】なお、ここでアクセス制御表１７のデータ配列の大きさを示す変数ＭＡＸの値を３と想定する。すなわちサーバ計算機１が同時に通信接続してサービス提供が可能なクライアント計算機５ｉは最大３台であると想定する。

【０１０３】クライアント計算機５ｉがサーバ計算機１にアクセスする。ここではサーバ計算機１のＴＣＰ／ＩＰの８０８０番で動作しているサーバに対してコネクションを受けたとする。サーバ計算機１ではメモリ１２上に展開されたサーバネットワークサービス部２１がＣＰＵ１１に制御され、ネットワーク制御を行なってサービスの受入れを待機する。サーバネットワークサービス部２１のソフトウェアとしてWWWサーバが想定される。

【０１０４】まず、サーバ管理者は１台のクライアント計算機５ｉにのみサーバ計算機１に対するアクセス要求の許可を与えるために、アクセス制御表管理部１８を介してアクセス許可フラグＡＦ（０）のみオンに設定したと想定する。

【０１０５】このとき、アクセス許可フラグＡＦ（０）がオフからオンに設定されるので、有効時間制御部１９は対応の有効時間Ｔ（０）に一定時間期間としてたとえば３０秒を設定して図５のフローチャートに従う以下の処理を実行する。

【０１０６】図５のフローチャートはＣＰＵ１１の制御により１秒ごとに起動される有効時間制御部１９による割込処理である。

【０１０７】有効時間制御部１９は、図５の割込処理が起動されると配列データである有効時間Ｔ（ｉ）の配列要素ポインタｉを１ずつインクリメントしながら、ポインタｉが配列の大きさＭＡＸ（＝３）となるまで、アクセス制御表１７中の有効時間Ｔ（ｉ）のうちその値が＞０であるものについて、値を１減算する（Ｓ２０～Ｓ２５）。

【０１０８】減算結果、有効時間Ｔ（ｉ）が０になり、かつ対応のクライアントアドレスＣＡ（ｉ）の内容が“空”であれば、対応するアクセス許可フラグＡＦ（ｉ）をオフに設定する。

【０１０９】その後、該割込処理は終了する。以上のように、サーバ管理者によりアクセス許可フラグＡＦ（ｉ）がオンに設定された後に、対応の有効時間Ｔ（ｉ）に設定された一定時間期間（３０秒）内に対応のクライアントアドレスＣＡ（ｉ）についてアドレス学習が行なわれなければ、アクセス許可フラグＡＦ（ｉ）は有効時間制御部１９により強制的にオンからオフに変更されて、サーバ計算機１へのクライアント計算機５ｉによるアクセス要求が一切許可されなくなる。

【０１１０】したがって、サーバ管理者が所望するクライアント計算機５ｉにのみアクセス要求を許可するためにアクセス許可フラグＡＦ（ｉ）をオンに設定し、その後有効時間Ｔ（ｉ）の一定時間期間内にクライアント計算機５ｉから送信されたアクセス要求がサーバ計算機１

で受信されて許可されれば、その後は該クライアント計算機５ｉについてはサーバ計算機１へのアクセス要求が許可されるようにアクセス制御表１７が設定される。

【０１１１】図４を参照して、サーバネットワークサービス部２１はサーバ計算機１の８０８０番のポート番号でサーバソケットをオープンし、コネクションを受付ける態勢に入る（Ｓ１）。

【０１１２】次に、クライアント計算機５ｉからサーバ計算機１に対してアクセス要求が送信されると、クライアント識別情報取得部２０はネットワークＩ／Ｏ１６を介して受理したパケット中のクライアント計算機５ｉのＩＰアドレスを取得して、これを変数ＣＡＤＲに設定する。この操作はＴＣＰ／ＩＰの基本であるので詳細は省略する（Ｓ２）。

【０１１３】次に、アクセス制御表管理部１８はポインタｉを０からＭＡＸまで１つずつインクリメントしながら次の処理を行なう。

【０１１４】アクセス制御表１７のクライアントアドレスＣＡ（ｉ）を検索し、クライアントアドレスＣＡ（ｉ）と変数ＣＡＤＲの内容が一致するものがあるか比較する（Ｓ４）。

【０１１５】一致するならば次のＳ５の処理へ、一致しないならばポインタｉを＋１インクリメントして次のクライアントアドレスＣＡ（ｉ）について同様に処理をする（Ｓ４１～）。

【０１１６】アクセス許可フラグＡＦ（ｉ）がオンならば（Ｓ５でＹＥＳ）、アクセス要求元のクライアント計算機５ｉにアクセス要求を許可してサービス提供を許可する（Ｓ６）。その後、Ｓ１の処理に移行する。アクセス許可フラグＡＦ（ｉ）がオンでないならば（Ｓ５でＮＯ）、アクセス要求したクライアント計算機５ｉに対しアクセス要求を許可しない旨の通知をしてサーバ計算機１によるサービスの提供を拒否する（Ｓ７）。その後、Ｓ１の処理に移行する。

【０１１７】アクセス要求したクライアント計算機５ｉから取得したＩＰアドレスに一致するクライアントアドレスＣＡ（ｉ）がなければ（Ｓ４２でＹＥＳ）、ポインタを１からＭＡＸまで１ずつインクリメントしながら次の処理を行なう。まず、クライアントアドレスＣＡ（ｉ）の内容が空であれば（Ｓ８でＹＥＳ）、該クライアントアドレスＣＡ（ｉ）に変数ＣＡＤＲの内容、すなわちアクセス要求したクライアント計算機５ｉから取得したＩＰアドレスを設定してアドレス学習し（Ｓ９）、対応の許可フラグＡＦ（ｉ）がオンなら（Ｓ１０でＹＥＳ）、アクセス要求したクライアント計算機５ｉにアクセス要求を許可してサービス提供を開始する（Ｓ１１）。一方、オフならば（Ｓ１０でＮＯ）、アクセス要求したクライアント計算機５ｉにアクセス要求の不許可を通知してサービス提供を拒否する（Ｓ１２）。その後は、再度次のアクセス要求を待つ状態（Ｓ１）に戻る。

【０１１８】一方、アクセス制御表１７に空であるクライアントアドレスＣＡ（ｉ）がなければ（Ｓ８２でＹＥＳ）、アクセス要求したクライアント計算機５ｉに対してアクセス要求の不許可を通知してサービス提供を拒否し（Ｓ１２）、次のアクセス要求を待つ状態（Ｓ１）に戻る。

【０１１９】図４のフローチャートに従う動作をより具体的に説明する。今、３台のクライアント計算機５ｉとしてクライアント計算機５０、５１および５２がネットワーク上にあって、それぞれ１２３．４５．６７．８９、１２３．４５．６７．９０、および１２３．１４５．６７．９１で示されるアドレスを識別情報として有していたとする。

【０１２０】まず、始めに図８のアクセス制御表１７のようにサーバ管理者により１つのアクセス許可フラグＡＦ（０）だけオン設定され、対応の有効時間Ｔ（０）に３０秒が設定されて、１台のクライアント計算機にのみアクセス要求の許可を与えるように設定したと想定する。

【０１２１】このとき、クライアント計算機５０が有効時間Ｔ（１）の３０秒以内にサーバ計算機１にアクセス要求したとすると、アクセス制御表１７の内容は図９のように更新されて、クライアント計算機５０はサーバ計算機１に対するアクセスが許可されて、サービス提供が開始される。

【０１２２】この場合の有効時間Ｔ（０）の経過に伴う許可フラグＡＦ（０）とクライアントアドレスＣＡ（０）の内容の変化が図６のタイミングチャートに示される。

【０１２３】続いて、クライアント計算機５１がサーバ計算機１にアクセス要求を送信するとアクセス制御表１７は図１０のように更新される。

【０１２４】したがって、クライアント計算機５１はサーバ計算機１においてアクセス要求が不許可となってサービス提供を受けることができない。

【０１２５】次に、図１（Ａ）のアクセス制御表管理部１８と有効時間制御部１９の動作を述べる。サーバ管理者は表示部１５に表示されたアクセス制御表１７のアクセス許可フラグＡＦ（１）を入力部１４を操作してオンに変更した後に、再度、クライアント計算機５１からアクセス要求が送信された場合のアクセス制御表１７の内容が図１１に示される。

【０１２６】次にサーバ管理者が同様にして図１２のようにアクセス制御表１７の３番目に登録されるアクセス許可フラグＡＦ（２）をオンに設定変更したとする。このとき、対応のクライアントアドレスＣＡ（２）は空であるので、対応の有効時間Ｔ（２）には３０秒がセットされる。

【０１２７】ここで、アクセス許可フラグＡＦ（２）がオン設定されてから、５０秒経過後にクライアント計算

機５２がサーバ計算機１にアクセス要求を送信する。この場合、アクセス制御表１７の有効時間Ｔ（２）は図１３のように０となって、対応の許可フラグＡＦ（２）は有効時間制御部１９によって既にオフとされているため、このアクセス要求は不許可となる。

【０１２８】この場合の、有効時間Ｔ（２）の経過に伴うアクセス許可フラグＡＦ（２）とクライアントアドレスＣＡ（２）の変化が図７のタイミングチャートに示される。

【０１２９】図１３では、クライアント計算機５２のアドレスがクライアントアドレスＣＡ（２）としてアドレス学習されるから、後で、サーバ管理者がアクセス制御表管理部１８を介して対応のアクセス許可フラグＡＦ（２）をオンに設定することで、クライアント計算機５２に対して以降アクセス要求が許可されるように設定することができる。

【０１３０】なお、本実施の形態では、クライアントアドレスＣＡ（ｉ）としてＴＣＰ／ＩＰのＩＰアドレスを用いたが、ＩＰアドレスをイーサーネットインターフェイスの固有のＭＡＣ（Media Access Control）アドレスに変換してから用いるようにしてもよい。

【０１３１】クライアント計算機５ｉの電源投入ごとにＩＰアドレスの異なる可能性のある方式としてＤＨＣＰによるアドレスの動的割当の場合がある（R. Droms RFC 1531 Dynamic Host Configuration Protocol参照）からである。

【０１３２】このようにアクセス制御表１７を用いた方法では、既にサーバ計算機１からアクセス要求が許可されてサービス提供を受けているクライアント計算機５ｉに優先的に排他的にサーバ計算機１のサービスの利用権が与えられ、かつ許可フラグＡＦ（ｉ）をオンにしてから一定時間以内にアクセス要求したクライアント計算機５ｉ以外はアクセス要求が許可されない。

【０１３３】このようなシステムの利用方法としては、サーバ計算機１とクライアント計算機５ｉの利用者が同一人物であり、サーバ計算機１側で、許可フラグＡＦ（ｉ）をオンに設定し、一定時間期間内にクライアント計算機５ｉからサーバ計算機１にアクセス要求を送信することによりクライアント計算機５ｉの識別情報をアクセス制御表１７にアドレス学習させて、以後、他のクライアント計算機５ｉのサーバ計算機１の利用が拒否されるようにできる。

【０１３４】なお、有効時間Ｔ（ｉ）の示す一定時間期間内にこのアドレス学習が完了できない場合は作業が中断したとみなして、再度、許可フラグＡＦ（ｉ）をオンにしなければならない。これにより、作業中断が発生しても、自動的に安全側に移行して、他の任意のクライアント計算機５ｉからサーバ計算機１が不正にアクセスされることが防止される。

【０１３５】上述した動作においては、予め定められた数のクライアント計算機５ｉに対して、最初にアクセス要求を送信しアクセス制御表１７のクライアントアドレスＣＡ（ｉ）の空欄を埋めることができたクライアント計算機５ｉのみ、それ以後サーバ計算機１の利用が可能になっていることがわかる。

【０１３６】このように、サーバ管理者は、クライアント計算機５ｉのアドレスをサービス許可パターンとしてサーバ計算機１に予め登録する必要がなく、簡単に特定のクライアント計算機５ｉからのアクセス要求のみを許可してサービス提供をするよう限定できる。

【０１３７】また、クライアント計算機５ｉとサーバ計算機１の管理者が同一人物であれば、サーバ計算機１でのサービス開始直後（アクセス許可フラグＡＦ（ｉ）がオンに設定された後）にクライアント計算機５ｉ側でサーバ計算機１がサービス提供可能であることを知る得るのは本人だけであり、サービス開始直後にサーバ計算機１に最初にアクセス要求を送信したクライアント計算機５ｉのみ、以後のサービス提供を受けることが可能になるという本方式では、アクセス制御においてユーザはアドレスの概念を知る必要がなくなって、使い勝手が向上する。

【０１３８】また、ユーザはクライアント計算機５ｉを用いてサーバ計算機１を利用するときにパスワードなどの入力が不要になり、使い勝手が向上する。また、クライアント計算機５ｉのアドレスはサーバ計算機１の不揮発メモリ１３に記憶されるので、サーバ計算機１が電源を切って、また再起動した場合でもアクセス制御表１７にアドレス学習された特定クライアント計算機５ｉのみに継続的にサービス提供することが可能となる。

【０１３９】また、図１４に示されたように入力部１４を介してアクセス制御表１７の内容を書換えることによって新たなクライアント計算機５ｉのアクセス要求を許可するように設定できる。たとえば、許可フラグＡＦ（ｉ）をオンに設定し、対応のクライアントアドレスＣＡ（ｉ）を空にしておくだけで、新たなクライアント計算機５ｉにサーバ計算機１のアクセス許可を与えることができる。

【０１４０】なお、上述した本実施の形態では、アクセス制御表１７に学習されたＩＰアドレスとアクセス要求とともに受理したＩＰアドレスとを照合しているが、これに限定されない。例えば、クライアント計算機側で任意に変更可能なＩＰアドレスとクライアント計算機側に固定に設定されて変更不可能なＭＡＣアドレスとを用いて照合するようにしてもよい。

【０１４１】つまり、アクセス制御表１７のＩＰアドレスとアクセス要求とともに受信したＩＰアドレス同士を照合して一致しても、アクセス制御表１７のＭＡＣアドレスとアクセス要求とともに受信したＭＡＣアドレス同士の照合結果が不一致であれば、アクセス要求元のクライアント計算機５ｉにアクセス要求を許可せずに、その

旨をユーザに通知するようにしてもよい。これによりアドレスの２重チエックが行なわれ、不正アクセスを確実に回避できる。この場合、図１４の画面ではＭＡＣアドレスの表示は省略される。

【０１４２】また、サーバ計算機１が個人が携帯するコンピュータであり、クライアント計算機５ｉがネットワークに固定して接続されたコンピュータである場合には、他の任意のクライアント計算機５ｉからサーバ計算機１が不用意にアクセスされて、サーバ計算機１の個人の情報が無断でアクセスされることが簡単かつ効果的に防止される。

【０１４３】今回か開示された実施の形態は全ての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】（Ａ）と（Ｂ）は、この発明の実施の形態によるサーバ計算機の機能構成とアクセス制御表とを示す図である。

【図２】この発明の実施の形態による通信ネットワークの構成図である。

【図３】図２のサーバ計算機のブロック構成図である。

【図４】この発明の実施の形態によるサーバ計算機におけるクライアント計算機からのアクセス要求の許可／不許可を制御するための手順を示すフローチャートである。

【図５】図４のフローチャートに従う処理に並行して実行される有効時間の減算処理のフローチャートである。

【図６】この発明の実施の形態によるサーバ計算機において、一定の有効時間内にクライアント計算機のアドレス学習が行なわれた場合の動作を示すタイミングチャートである。

【図７】この発明の実施の形態によるサーバ計算機において、一定の有効時間内にクライアント計算機のアドレス学習が行なわれなかった場合の動作を示すタイミングチャートである。

【図８】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第１例を示す図である。

【図９】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第２例を示す図である。

【図１０】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第３例を示す図である。

【図１１】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第４例を示す図である。

【図１２】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第５例を示す図である。

【図１３】この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第６例を示す図である。

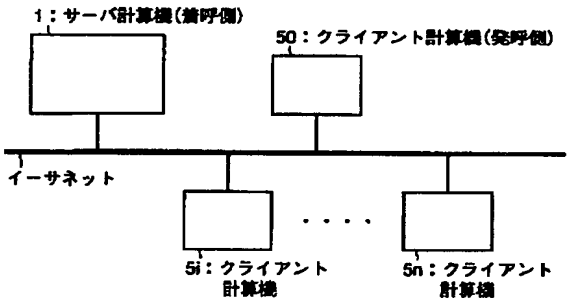
【図１４】この発明の実施の形態によるアクセス制御表の書換を説明する図である。

【符号の説明】

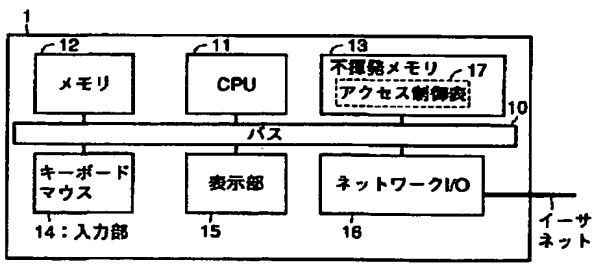
１　サーバ計算機
５ｉ　クライアント計算機（ｉ＝０、１、２、…、ｎ）
１１　ＣＰＵ
１２　メモリ
１３　不揮発メモリ
１４　入力部
１５　表示部
１７　アクセス制御表
１８　アクセス制御表管理部
１９　有効時間制御部
２０　クライアント識別情報取得部
ＡＦ（ｉ）　アクセス許可フラグ
Ｔ（ｉ）　有効時間
ＣＡ（ｉ）　クライアントアドレス

なお、各図中同一符号は同一または相当部分を示す。

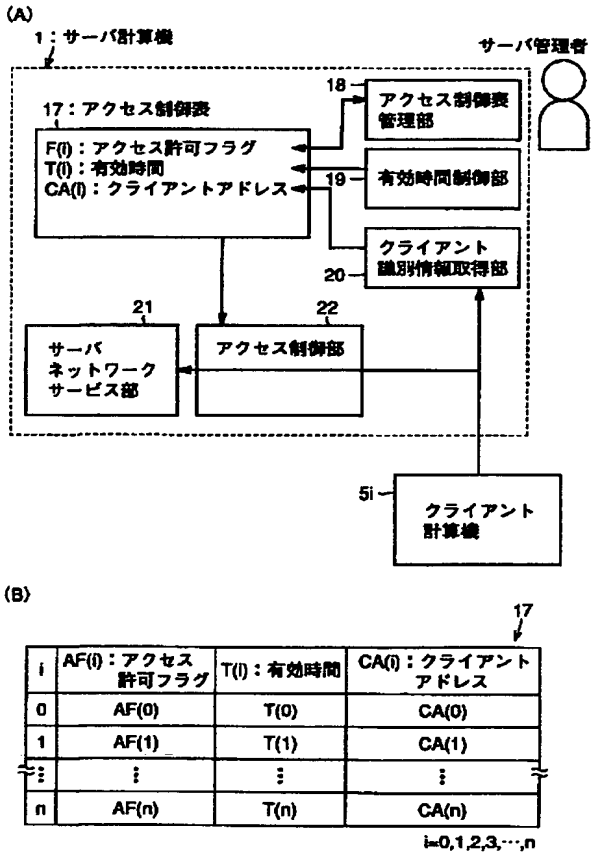
【図２】



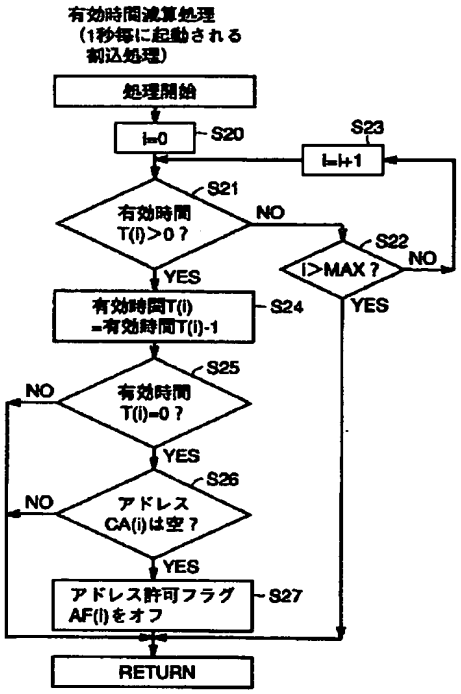
【図３】



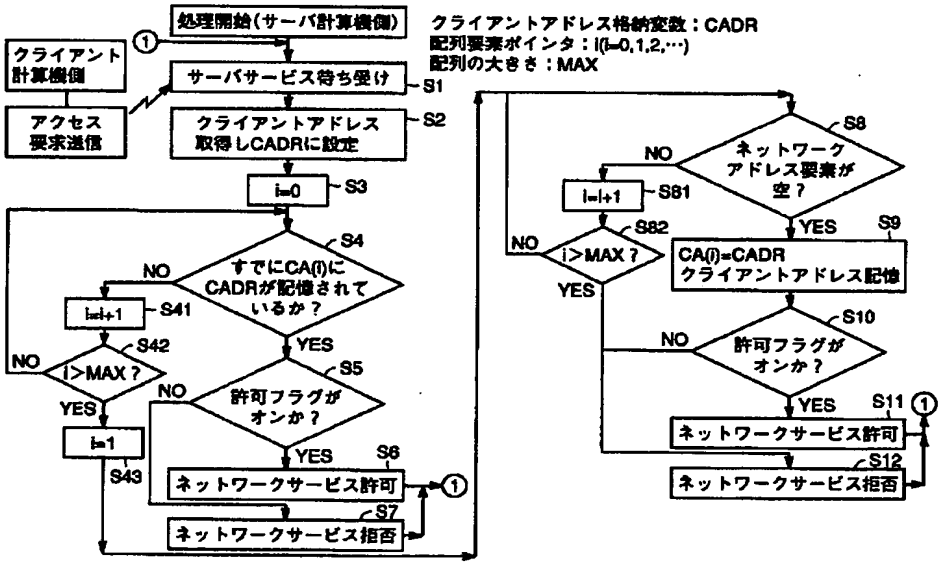
【図１】


(A)
1：サーバ計算機
サーバ管理者
17：アクセス制御表
F(i)：アクセス許可フラグ
T(i)：有効時間
CA(i)：クライアントアドレス
18
アクセス制御表管理部
19
有効時間制御部
20
クライアント識別情報取得部
21
サーバネットワークサービス部
22
アクセス制御部
5i
クライアント計算機
(B)
17
i
AF(i)：アクセス許可フラグ
T(i)：有効時間
CA(i)：クライアントアドレス
0
AF(0)
T(0)
CA(0)
1
AF(1)
T(1)
CA(1)
n
AF(n)
T(n)
CA(n)
i=0,1,2,3,…,n

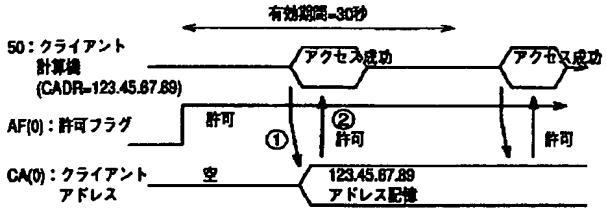
【図５】


有効時間減算処理
（1秒毎に起動される割込処理）
処理開始
i=0
S20
S21
有効時間 T(i)>0？
NO
YES
S22
i>MAX？
NO
YES
S23
i=i+1
有効時間T(i) =有効時間T(i)-1
S24
S25
有効時間 T(i)=0？
NO
YES
S26
アドレス CA(i)は空？
NO
YES
アドレス許可フラグ AF(i)をオフ
S27
RETURN

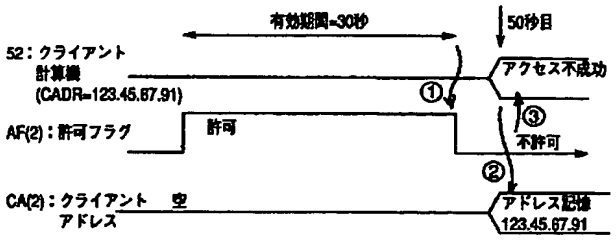
【図４】


処理開始(サーバ計算機側)
クライアント計算機側
①
サーバサービス待ち受け
S1
アクセス要求送信
クライアントアドレス取得しCADRに設定
S2
i=0
S3
S4
すでにCA(i)にCADRが記憶されているか？
NO
YES
i=i+1
S41
S42
i>MAX？
NO
YES
i=1
S43
S5
許可フラグがオンか？
NO
YES
S6
ネットワークサービス許可
①
S7
ネットワークサービス拒否
クライアントアドレス格納変数：CADR
配列要素ポインタ：I(i=0,1,2,…)
配列の大きさ：MAX
S8
ネットワークアドレス要素が空？
NO
YES
i=i+1
S81
S82
i>MAX？
NO
YES
S9
CA(i)=CADR
クライアントアドレス記憶
S10
許可フラグがオンか？
NO
YES
S11
①
ネットワークサービス許可
S12
ネットワークサービス拒否

【図６】



【図７】



【図８】

17

	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	30	
1	オフ	0	
2	オフ	0	

【図９】

17

	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	25	123.45.67.89
1	オフ	0	
2	オフ	0	

【図１０】

17

	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	25	123.45.67.89
1	オフ	0	123.45.67.90
2	オフ	0	

【図１１】

17

	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	25	123.45.67.89
1	オン	0	123.45.67.90
2	オフ	0	

【図１２】

17

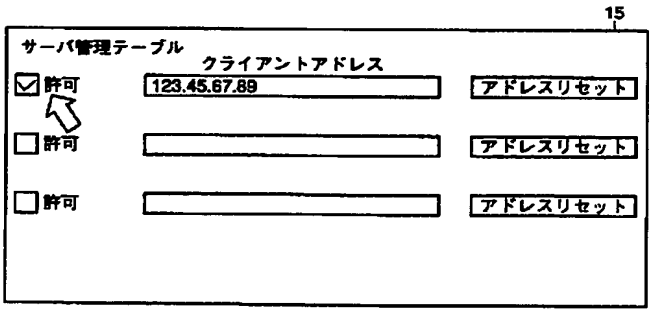
	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	25	123.45.67.89
1	オン	0	123.45.67.90
2	オン	30	

【図１３】

17

	F(i)：アクセス許可フラグ	T(i)：有効時間	CA(i)：クライアントアドレス
0	オン	25	123.45.67.89
1	オン	0	123.45.67.90
2	オフ	0	123.45.67.91

【図１４】



フロントページの続き

(54)【発明の名称】 通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置、ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体